METU, Spring 2014, Math 504.

Final (May 30)

1. **(12 pts)** Let $T : V \to V$ be a linear transformation on a finite dimensional vector space V over a field $\mathbf{F}$. Let $\mathbf{F}[T]$ be the ring of all linear operators on V that can be expressed as polynomials in T with coefficients from F. Assume that no nonzero proper subspace of V is mapped into itself by T. Show that $\mathbf{F}[T]$ is a field and $[\mathbf{F}[T] : F] = \dim_F V$.

   Solution: The vector space V can be made into a $\mathbf{F}[x]$-module via $x \cdot v = Tv$. Being finitely generated, V can be decomposed as $V = V_{\text{tors}} \oplus V_{\text{free}}$. Since V is finite dimensional, the free part V_{free} must be trivial. As a result we have

   $$V \cong \mathbf{F}[x]/(p_1)^{n_1} \oplus \cdots \oplus \mathbf{F}[x]/(p_k)^{n_k}$$

   for some irreducible polynomials $p_i \in \mathbf{F}[x]$ and natural numbers n_i. Suppose that no nonzero proper subspace of V is mapped into itself by T. It follows that $V \cong \mathbf{F}[x]/(p_1)$ where p_1 is of degree $n = \dim_{\mathbf{F}} V$. Consider the evaluation map $\varphi : \mathbf{F}[x] \to \mathbf{F}[T]$ defined by $\varphi(f(x)) = f(T)$. This map is a surjective ring homomorphism. Moreover its kernel is precisely the ideal generated by p_1. Therefore $\mathbf{F}[T]$ is a field and $[\mathbf{F}[T] : \mathbf{F}] = \dim_{\mathbf{F}} V$

2. **(12 pts)** Let R be a principal ideal domain. Determine all finitely generated R-modules M such that $M \otimes_R M \cong M$.

   Solution: Let M be a cyclic R-module generated by $m \in M$. Then it is easy to see that $M \otimes_R M \cong M$ by the isomorphism $r_1 m \otimes r_2 m \mapsto r_1 r_2 m$. We want to justify that any finitely generated R-module M such that $M \otimes_R M \cong M$ is cyclic. The structure of M is given by

   $$M \cong R^n \oplus R/(a_1) \oplus \cdots \oplus R/(a_k)$$

   for some natural number n and $a_i \in R$ such that $a_1 | \dots | a_k$. Recall that

   $$(A \oplus B) \otimes_R C \cong (A \otimes_R C) \oplus (B \otimes_R C).$$

   From this fact, we see that $n \leq 1$. Moreover we have $M \otimes_R R/(a_i) \cong M/(a_i)M$ for each $i \in \{1, \dots, k\}$. Thus either $M \cong R$ or the free part of M is trivial. Now suppose that the free part of M is trivial. If $i \leq j$, then we have $R/(a_i) \otimes R/(a_j) \cong R/(a_i)$ since $\gcd(a_i, a_j) = a_i$. It follows that M is cyclic and $M \cong R/(a_i)$.

3. Let F/K be a finite extension of fields. The intermediate fields E_1 and E_2 are said to be linearly disjoint if $[E_1 E_2 : K] = [E_1 : K][E_2 : K]$ where $E_1 E_2$ is the composite field.

   - **(4 pts)** If $[E_1 : K]$ and $[E_2 : K]$ are relatively prime, then show that E_1 and E_2 are linearly disjoint over K.

     Solution: The composite extension $E_1 E_2$ is a finite extension of K of dimension less than or equal to $[E_1 : K][E_2 : K]$. To see this, let X_i be a basis for E_i where

$i = 1, 2$. Then any element in E_1E_2 can be written as a K-linear combination of elements from $\{x_1x_2 | x_1 \in X_1, x_2 \in X_2\}$.

On the other hand $[E_1E_2 : K] = [E_1E_2 : E_i][E_i : K]$ for each i by the tower law. Since $[E_1E_2 : K]$ is divisible by both $[E_1 : K]$ and $[E_2 : K]$, which are relatively prime, we must have $[E_1E_2 : K] \geq [E_1 : K][E_2 : K]$. This finishes the proof.

- **(6 pts)** Give an example with $[E_1 : K] = 2 = [E_2 : K]$ to show that there are linearly disjoint fields without having relatively prime degrees.

  Solution: Let $E_1 = \mathbf{Q}(i)$ and $E_2 = \mathbf{Q}(\sqrt{2})$. It is easy to see that $\zeta_8 = \exp(2\pi i/8)$ is an element of $\mathbf{Q}(i, \sqrt{2})$. Since $\mathbf{Q}(\zeta_8) \subset E_1E_2$ and $[\mathbf{Q}(\zeta_8) : \mathbf{Q}] = \varphi(8) = 4$, we conclude that E_1 and E_2 are linearly disjoint.

- **(6 pts)** If $F = \mathbf{F}_q$ and $K = \mathbf{F}_p$ then find a sufficient and necessary condition so that the intermediate fields E_1 and E_2 are linearly disjoint.

  Solution: Let $n_i = [E_i : \mathbf{F}_p]$ for $i = 1, 2$. By the first part, we see that the condition $\gcd(n_1, n_2) = 1$ is sufficient for being linearly disjoint. Now we will show that this condition is necessary in the case of finite fields. Assume otherwise and let $\gcd(n_1, n_2) = d > 1$. The intermediate field E_i is the splitting field of $x^{p^{n_i}} - x$. Let e be least common multiple of n_1 and n_2. The composite field E_1E_2 is contained in the splitting field of $x^{p^e} - x$ which is of dimension e over $\mathbf{F}_p$. However $e = n_1n_2/d$ and it is strictly less than n_1n_2.

4. **(10 pts)** Let F/K be a Galois extension and set $G = \mathrm{Aut}_K F$. Let $f(x) \in K[x]$ be a monic polynomial that splits over F and let $S \subseteq F$ be the set of roots of $f(x)$. Prove that $f(x)$ is a power of an irreducible polynomial in $K[x]$ if and only if G acts transitively on S.

   Solution:($\Rightarrow$) Suppose that $f(x) = p(x)^n$ for some irreducible polynomial $p(x)$ in $K[x]$. Let u, v be two elements of S. There exist an isomorphism of fields $K(u) \cong K(v)$ which maps u onto v. Moreover this isomorphism can be extended to an automorphism of F which contains the splitting field of $p(x)$ over K. Thus there exists $\sigma \in G$ such that $\sigma(u) = v$.

   ($\Leftarrow$) Suppose that G acts transitively on S. Let u, v be two elements of S. Then there exists $\sigma \in G$ such that $\sigma(u) = v$. As a result $\sigma|_{K(u)}$ is an isomorphism between $K(u)$ and $K(v)$ fixing K elementwise. Let $p(x) \in K[x]$ be the irreducible polynomial of $u \in F$. Observe that $p(v) = p(\sigma(u)) = \sigma(p(u)) = 0$. Thus each element in S must be a root of $p(x)$. Therefore $f(x)$ is a power of an irreducible polynomial in $K[x]$.

5. **(10 pts)** Let F/K be a finite Galois extension and let $F = K(\alpha)$ for some $\alpha \in F$. Suppose that there is $\sigma \in \mathrm{Aut}_K F$ such that $\sigma(\alpha) = 1/(1 - \alpha)$. Prove that $[F : K]$ is a multiple of three and $[K(\alpha + \sigma(\alpha) + \sigma^2(\alpha)) : K] = [F : K]/3$.

   Solution: Observe that $\sigma^3(\alpha) = \alpha$. Since α is an element generating the Galois extension F/K, the automorphism σ is of order 3. According to the fundamental theorem of Galois theory the fixed field of the subgroup $\langle \sigma \rangle$ is of index 3 in F. Note that the element $\beta = \alpha + \sigma(\alpha) + \sigma^2(\alpha)$ remains fixed under the automorphism σ.